主要内容

一、 概述（续）

◆网络安全体系结构

- ❖安全威胁（攻击）
- ❖安全服务
- ❖安全机制

◆网络安全标准

二、密码技术应用

◆密码学基本概念

网络安全体系结构（OSI）

◆OSI安全体系结构：OSI Security Architecture

- ❖ 国际电信联盟ITU-T X.800 "Security Architecture for OSI"

◆一种系统的方法，定义和提供安全需求

◆国际标准

- ❖提供概念模型

◆信息安全的三个方面

- ❖安全攻击 security attack
- ❖安全机制 security mechanism
- ❖安全服务 security service

基本概念

◆攻击attack

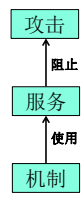
- ❖安全攻击：任何破坏信息安全的行为。(e.g., stealing information).

◆机制mechanism

- ❖安全机制：用来检测detect、阻止prevent安全攻击，或从攻击中恢复recover的机制。(e.g., encryption)

◆服务service

- ❖安全服务：增强数据处理系统和信息传输的安全性的服务。安全服务可以利用一个或多个安全机制。 (e.g., SSL for Web browsers and servers).



威胁 vs. 攻击

◆两个概念

- ❖威胁 *threat* – a potential for violation of security
- ❖攻击 *attack* – an assault on system security, a deliberate attempt to evade security services

网络安全威胁来自哪里

- 内因
  - 人们的认识能力和实践能力的局限性
  - 系统软件规模的庞大
  - 系统自身的脆弱性
    - 网络的开放性
    - 黑客（Hacker）及病毒等恶意程序的攻击
    - 系统平台系统软件的自身缺陷
    - TCP/IP分层体系结构的脆弱性
    - 操作系统及数据库的脆弱性
  - 网络误用/滥用
  - 没有良好的管理机制

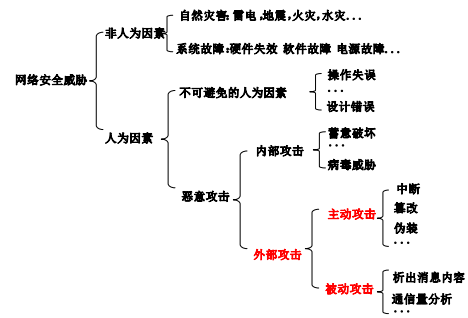
安全威胁来自哪里

- 外因

国家安全威胁	信息战士	减小决策空间、战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事，经济信息
共同威胁	恐怖分子	破坏公共秩序，制造混乱，发动政变
	工业间谍	掠夺竞争优势，恐吓
	犯罪团伙	施行报复，实现经济目的，破坏制度
局部威胁	社会型黑客	攫取金钱，恐吓，挑战，获取声望
	娱乐型黑客	以吓人为乐，喜欢挑战

例：网络存在的安全威胁

网络安全威胁分类

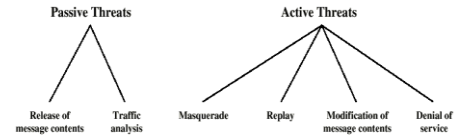


例：网络威胁统计

- 国外
  - Computer Emergency Response Team
    - www.us-cert.gov
  - 安全研究机构www.sans.org
  - 赛门铁克的漏洞库 https://www.securityfocus.com/
  - 美国国家信息安全漏洞库 https://nvd.nist.gov/
- 国内
  - 国家互联网应急中心 http://www.cert.org.cn/
  - 国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD） http://www.cnvd.org.cn/
- 网络安全厂商

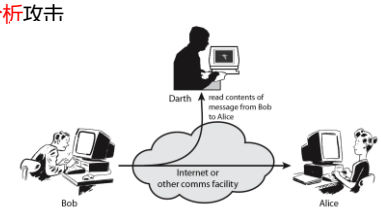
安全威胁/攻击

- 安全威胁/攻击(Security Threats/Attack)
  - 被动攻击Passive Threats
  - 主动攻击Active Threats



网络攻击方式：被动攻击

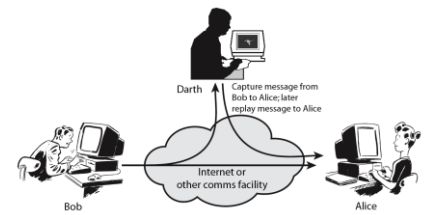
- 被动攻击
  - 消息内容泄露：窃听或者偷窥
  - 流量分析攻击



应对被动攻击：防范（如加密）

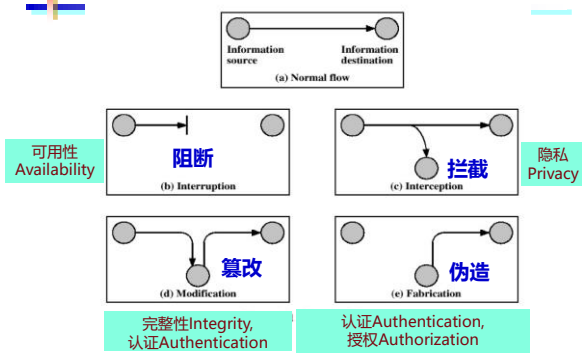
网络攻击方式：主动攻击

- 主动攻击
  - 指攻击者对某个连接中的数据进行各种处理(阻断、拦截、伪造、重放、篡改、拒绝服务等)



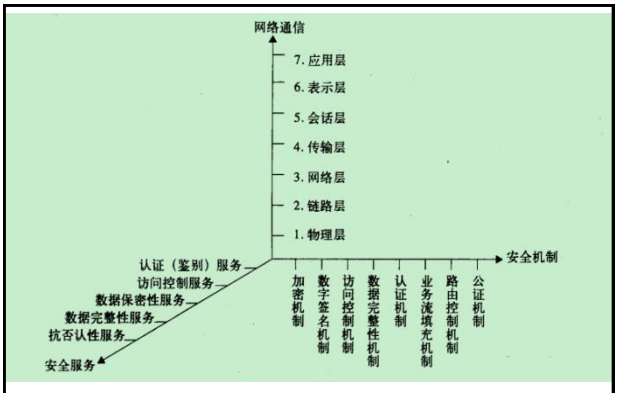
应对主动攻击：检测和恢复

主动攻击的几种类型



OSI安全体系结构

- 1988年，ISO发布ISO7498-2标准，，基于OSI参考模型之上的网络安全体系结构
  - 定义5类安全服务，8种安全机制
  - 确定了安全服务与安全机制之间的关系
- ITU-T将ISO7498-2标准作为X.800建议书



什么是安全服务?

- X.800的定义
  - 由通信开放系统的协议层提供的，并能确保系统或数据传输足够安全的服务
  - 5类14种特定服务（参考书1，表1.2）
- RFC4949 Internet Security Glossary, Version 2
  Internet安全术语表 （课外阅读）
  - 由系统提供的对系统资源进行特定保护的处理或通信服务。

security service:

A processing or communication service that is provided by a system to give a specific kind of protection to system resources.

Internet安全术语（RFC4949）

安全服务实现安全策略
安全机制实现安全服务

Security services implement security policies, and are implemented by security mechanisms.

--RFC4949

Internet安全术语（RFC4949）

- 攻击方（威胁代理）
- 攻击
- 对策
- 风险
- 安全策略
- 系统资源（资产）
- 威胁
- 脆弱性

Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

RFC 4949, Internet Security Glossary

安全服务（X.800）

- 五类可选的安全服务
  - 认证/鉴别Authentication：鉴别用于保证通信的真实性
  - 访问控制Access Control：防止对网络资源的非授权访问
  - 数据机密性Data Confidentiality：保护数据以防止被动攻击
  - 数据完整性Data Integrity：保证所接收的消息未经复制、篡改、插入、重排或重放，既用于对付主动攻击
  - 不可否认Non-Repudiation：防止通信双方中的某一方抵赖所传输的消息

安全服务（X.800）

- 认证 Authentication
  - 用户登录认证
  - 消息认证
- 访问控制access control 和授权 Authorization
  - 防止资源被误用
- 机密性和隐私 （Confidentiality，Privacy)
- 完整性（Integrity）
  - 没有被修改或删除
- 可用性Availability (持久性，不可中断)
  - 例如：拒绝服务（DoS）攻击； 病毒破坏文件
- 不可否认性Non-repudiation
- 标准
  - ISO X.800：Security architecture for Open Systems Interconnection for CCITT application
  - IETF RFC 4949：Internet Security Glossary

安全机制

- 特点
  - 从安全攻击中检测、阻止或恢复的特征
    Feature designed to detect, prevent, or recover from a security attack
- 多种机制
  - 特定安全机制：特定协议层上执行
  - 普适安全机制：不指定特定OSI安全服务，跨层执行
- 安全服务可以由多种安全机制联合提供
  - 注意：*no single mechanism that will support all services required*
- 基础
  - 密码技术

安全机制（X.800）

- 特定安全机制:
  - Encipherment 加密, digital signatures 数字签名
  - access controls 访问控制
  - data integrity 数据完整性
  - authentication exchange 认证交换
  - traffic padding 流量填充, routing control 路由控制
  - notarization公证
- 普适安全机制:
  - trusted functionality可信功能
  - security labels安全标签
  - event detection事件检测
  - security audit trails安全审计跟踪
  - security recovery安全恢复

安全服务和机制的关系（表1.4）

	Mechanism							
Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

安全产品

安全产品是安全机制的载体

- 防火墙（Firewall）
- 入侵检测系统（Intrusion Decection System，IDS）
- 恶意软件防护

恶意软件Malware的类型

- 病毒Viruses
  - Code that attaches itself to programs, disks, or memory to propagate itself
- 蠕虫Worms
  - Installs copies of itself on other machines on a network, e.g., by finding user names and passwords
- 木马 Trojan horses
  - Pretend to be a utility. Convince users to install on PC
- Rootkit
  - 监控程序，Gets “root” (admin) privilege
- Spyware
- Key Loggers，Hoax，Trap Door，Logic Bomb，Zombie，...

计算机病毒（Computer Virus）

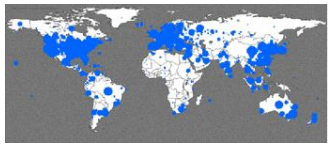
- 《中华人民共和国计算机信息系统安全保护条例》中的相关定义
  - “指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。
- 病毒必须满足两个条件：
  - 能自行执行。它通常将自己的代码置于另一个程序的执行路径中。
  - 能自我复制。例如，它可能用受病毒感染的文件副本替换其他可执行文件。
- 病毒既可以感染桌面计算机也可以感染网络服务器。
- 病毒往往还具有很强的感染性，一定的潜伏性，特定的触发性和很大的破坏性等。

蠕虫Worm

- 通过网络连接进行传播的恶意程序
  - 它具有病毒的一些共性，如传播性、隐蔽性、破坏性等等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），对网络造成拒绝服务，以及和黑客技术相结合。
  - 典型的蠕虫病毒有尼姆达、震荡波、熊猫烧香等。
- 历史
  - 1998年11月， Morris 蠕虫通过邮件服务器进行传播
  - 2001年， “Code Red” 蠕虫 攻击了Internet上约 360,000台 PC机。感染数量每37分钟翻一番。
  - 2004年， “Witty” 蠕虫感染特定网络安全产品：ISS “Black Ice” and “Real Secure.” 45分钟内感染了大量系统.

蠕虫Worm

- 例：2003年1月25日，SQL Slammer（又名：Sapphire爆发，它是曾经出现过的传播速度最快的蠕虫，每隔8.5秒的时间它所感染的主机的数目就要翻一番，在10分钟的时间内它就感染了近90%的脆弱性主机。该蠕虫利用的是SQL服务器或MSDE 2000中包含的缓冲区溢出漏洞。



Spread of Sapphire virus, after 38 minutes.

木马（Trojan Horse）

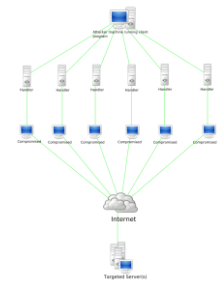
- 木马正是指那些表面上是有用的软件、实际目的却是危害计算机安全并导致严重破坏的计算机程序。
  - 是一种基于远程控制的黑客工具，具有欺骗性、隐蔽性和非授权性的特点。
  - 隐蔽性：是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，也难以确定其具体位置；
  - 非授权性：是指一旦控制端与服务端连接后，控制端将窃取到服务端的很多操作权限，如修改文件，修改注册表，控制鼠标，键盘，窃取信息等等。

Rootkit

- Rootkit是一种特殊的恶意软件
- 是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，比较多见到的是Rootkit一般都和木马、后门等其他恶意程序结合使用。
- Rootkit通过加载特殊的驱动，修改系统内核，进而达到隐藏信息的目的。

僵尸网络Botnet

- 演化：二十世纪末期，蠕虫演化为僵尸网络 "Bot" (for Robot)
  - 2008年11月，“Conficker” 感染了大约1千万台计算机；每天发送约10亿封 垃圾邮件和钓鱼邮件
- 作用
  - 发送垃圾邮件（Spam）和钓鱼邮件（ Phishing ）
  - 控制其他计算机
  - 发动攻击：如分布式拒绝服务攻击(DDOS)

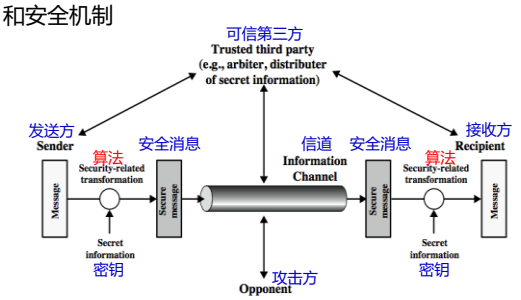


网络安全模型

- 网络加密安全模型
- 网络访问安全模型

网络加密安全模型

- 网络加密安全模型由三部分构成：参与者、信息通道和安全机制

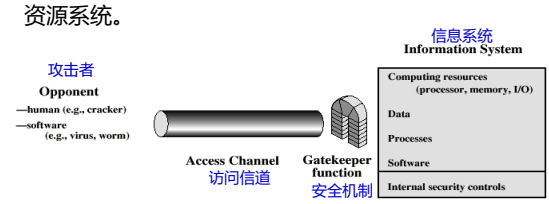


网络安全模型

- 设计安全服务的需求
  1. 算法：design a suitable algorithm for the security transformation
  2. 产生密钥：generate the secret information (keys) used by the algorithm
  3. 分发密钥：develop methods to distribute and share the secret information
  4. 安全协议：specify a protocol enabling the principals to use the transformation and secret information for a security service

网络访问安全模型

- 网络访问安全模型保护系统资源免受非授权的访问。模型由四部分构成：攻击者、访问信道、安全机制和资源系统。



相关标准化组织

- NIST（美国国家标准与技术研究院，National Institute of Standards and Technology ）
  - 加密标准，如AES, SHA
- Internet Engineering Task Force (IETF)
  - Internet标准：RFCxxxx
- ITU标准
  - X.509 Certificates
- IEEE
  - 802.3-Ethernet, 802.11 - Wireless LAN
- International Organization for Standardization (ISO)
- Department of Defense, Nat. Computer Security Center
  - Orange Book: Class A1, B3, C1, C2, ...
- 事实标准
  - De Facto (PGP email security system, Kerberos-MIT)
- 中国国家标准（GB）
  - GB/T9387.2-1995 GB/T 9387.2-1995 信息处理系统 开放系统互连基本参考模型 第2部分:安全体系结构

安全标准分类

- 类别
  - 密码标准
    - DES等
  - 协议标准
    - SSL等
  - 信息安全管理标准
    - ISO 17799等
  - 安全评估标准
    - TCSEC-ITSEC-CC等

研究资源

- 网络安全相关的国际会议
  - IEEE Symposium on Security and Privacy
  - ACM Conference on Computer and Communications Security
  - Usenix Security Symposium
  - ISOC Network and Distributed System Security Symposium
  - Annual Computer Security Applications Conference

二、密码技术应用

密码学基本概念

对称密码体系

公钥密码体系

密码学概述

- 密码学是一门古老而深奥的学科
  - 只在很小的范围内使用，如军事、外交、情报等部门
- 计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科
- 是网络空间安全主要研究方向之一
- 是很多安全机制的基础

密码学概述（续）

- 理论基础
  - 数论中许多基本内容，如同余理论、中国剩余定理（CRT）、高次剩余理论等，在新型密码体制、密钥分配与管理、数字签名、身份认证等方面有直接的应用。
  - 近代数学：近代数学在现代密码研究中的应用包括群论，有限域上椭圆曲线理论，多项式理论与迹函数理论，陷门单向函数 等。
- 密码学的两个分支
  - 密码编码学：主要研究对信息进行变换，以保护信息在信道的过程中不被敌手窃取、解读和利用的方法 。
  - 密码分析学：主要研究如何分析和破译密码，也称为密码攻击

密码学的发展

- 第一个阶段（1949年之前）
  - 传统密码学阶段，即古典密码学阶段，该阶段基本上依靠人工和机械对信息进行加密、传输和破译
  - 罗马国王Julius Caesare（恺撒）就开始使用目前称为“恺撒密码”的密码系统
- 第二阶段（1949～1975年）
  - 是计算机密码学阶段，该阶段又可细分为两个阶段
    - 使用传统方法的计算机密码学阶段
    - 使用现代方法的计算机密码学阶段
- 在20世纪70年代，密码学的研究出现了两大成果
  - 1977年美国国家标准局（NBS）颁布的联邦数据加密标准（DES）
  - 1976年由 Diffie 和 Hellman 提出的公钥密码体制的新概念

2015年 图灵奖（A.M. Turing Award）

- 2015年图灵奖的得主：Sun Microsystems公司前首席安全官Whitfield Diffie和斯坦福大学电气工程系名誉教授Martin Hellman
  - 1976年，开创性论文“密码学新方向”（New Directions in Cryptography）
  - 提出了公钥加密和数字签名的构想，奠定了公钥密码交换系统的基础，被广泛应用于当前网络通信。-- “Diffie-Hellman 协议”

术语与定义（1）

（1）消息（Message）

消息是指用语言、文字、数字、符号、图像、声音或其组合等方式记载或传递的有意义的内容。在密码学里，消息也称为信息。

（2）明文（Plaintext）

未经过任何伪装或隐藏技术处理的消息称为明文。

（3）加密（Encryption）

利用某些方法或技术对明文进行伪装或隐藏的过程称为加密。

（4）密文（Cipher Text）：被加密的消息称为密文。

（5）解密（Decryption）：将密文恢复成原明文的过程或操作称为解密。解密也可称为脱密。

术语与定义（2）

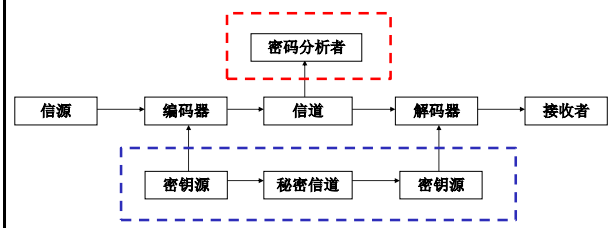
（6）加密算法（Encryption Algorithm）：将明文消息加密成密文所采用的一组规则或数学函数。

（7）解密算法（Decryption Algorithm）：将密文消息解密成明文所采用的一组规则或数学函数。

（8）密钥（Key）：进行加密或解密操作所需要的秘密参数或关键信息。在密码系统中，密钥分为私钥与公钥两种。私钥指必须保密的密钥，公钥指可以向外界公开的密钥。

（9）密码系统（Cryptosystem）：一个密码体制或密码系统是指由明文空间、密文空间、密钥空间、加密算法以及解密算法组成的一个多元素集合体。

密码系统的模型–组成



密码系统的安全性

- 密码分析和密码攻击
  - 非授权者：通过各种方法来窃听、干扰信息
  - 非授权者借助窃听到的密文以及其他一些信息通过各种方法推断原来的明文甚至密钥
- 无条件的安全性
  - 若攻击者无论得到多少密文也求不出确定明文的足够信息,这种密码系统就是理论上不可破译的,即密码系统具有无条件安全性(或完善保密性)

无条件安全性

- Unconditionally secure，是否绝对安全?
  - 永不可破：理想情况
  - 理论上不可破，密钥空间无限，在已知密文条件下，方程无解
  - 除了**一次一密**，所有加密算法都不是无条件安全的

密码系统的安全性（续）

- 实际安全性
  - 若一个密码系统原则上虽可破译，但为了由密文得到明文或密钥却需付出十分巨大的计算，而不能在希望的时间内或实际可能的经济条件下求出准确的答案，这种密码系统就是实际不可破译的，或称称该密码系统具有计算安全性
- Computationally secure，计算安全?
  - 破解的代价超过了加密信息本身的价值
  - 破解的时间超过了加密信息本身的有效期

影响安全性的几个因素

- 算法强度
  - 算法的强度越高，攻击者越难破译
- 其它因素
  - 其他的各种非技术手段（如管理的漏洞，或是某个环节无意暴露了敏感信息等）来攻破一个密码系统

密码攻击类型

- 惟密文攻击 Ciphertext only (hardest)
  - 分析者知道一个或一些密文的情况下，企图得到明文或密钥等敏感信息。
  - 容易抵抗。注意消息中的固定明文模式。
- 已知明文攻击 Ciphertext and corresponding Plaintext
  - 分析者知道一些明文及对应的密文的对应关系
- 选择明文攻击 Chosen Plaintext
  - 分析者获得更大机会接近密码系统，可以选择一些对攻击有利的特定明文，并得到对应的密文，以及在此基础上进行密码的破译

密码攻击类型 （续）

- 选择密文攻击 Chosen Ciphertext
  - 与选择明文攻击相反，分析者可以选择性地知道一些攻击有利的特定密文，并得到对应的明文
- 选择文本Chosen Text
  - 选择明文或密文进行加/解密

密码系统的安全需求

- 密码系统的密钥空间必须足够地大
- 加密与解密过程必须是计算上可行的
  - 能够被方便地实现与使用
- 整个密码系统的安全性系于密钥上
  - 即使密码方案被公布，在密钥不泄露的情况下，密码系统的安全性也可以得到保证

加密方法分类

三种分类方法:

- 从明文到密文的变换
  - 替换(substitution)
  - 置换(transposition)
  - ……
- 密钥的数目
  - 对称、单钥加密法
  - 公钥、双钥加密
- 明文的处理方式
  - 分组加密（块加密算法）
  - 流方式加密

作业

- 阅读RFC4949, 理解网络安全基本概念
- 加密算法的两个基本要素是什么?
- 问题：某人用自己的密钥加密一个随机比特串（与密钥长度相同），采用异或运算，并通过通道发送结果。接收方得到密文后，和自己手里的密钥进行异或运算，并发回。如果某人接收到的这个是原始比特串，则证实两人拥有同一密钥。这种方法没有在信道上传递过密钥，是否能保证密钥的安全？这个方案是否有缺陷?
- 攻击密码的两个通用方法是什么?
- 分组密码和流密码的区别是什么?